CHAPTER 10

インタラクティブ検出モードの使用方法

ゾーン異常検出をイネーブルにすると、Cisco Traffic Anomaly Detector Module（Detector モジュール）では、ゾーンのトラフィックが分析されて、超過しているポリシーのしきい値が検索されます。ポリシーのしきい値を超過したことを検出すると、トラフィックを分析し、トラフィックを処理するための動的フィルタのセットを作成します。Detector モジュールは、推奨事項を使用して、動的フィルタを自動またはインタラクティブのどちらでもアクティブにできます。この章では、インタラクティブ検出モードについて説明します。この章は、次の項で構成されています。

インタラクティブ検出モードについて

Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃が開始されると、Detector モジュールのポリシーは動的フィルタを作成します。ゾーンがインタラクティブ検出モードである場合、Detector モジュールはこのような動的フィルタを自動的にアクティブにせず、どのようなアクションを取るかをユーザが決定するのを待ちます。ユーザの決定を待つフィルタは、保留動的フィルタと呼ばれます。Detector モジュールは、保留動的フィルタを推奨事項に従って生成したポリシーに応じて分類します。この推奨事項は、保留フィルタの要約と、保留動的フィルタの作成の元になるポリシーの名前、ポリシーのアクティベーションの原因となったトラフィック異常に関するデータ、保留動的フィルタの数、および推奨アクションについての情報を提供します。ユーザは、どの保留動的フィルタを受け入れるか、無視するか、または自動アクティベーションに向けるかを決定します。インタラクティブ検出モードは、攻撃の進行中に取るアクションを、より詳細に制御できます。

Detector モジュールは、インタラクティブ検出モードになっている限り、保留動的フィルタの生成を続けます。ゾーンの異常検出中は、いつでもインタラクティブ検出モードをアクティブにできますが、Detector モジュールがインタラクティブ検出モードで、ゾーンに対する DDoS 攻撃が進行中である場合に限り、推奨事項およびその保留動的フィルタを表示できます。インタラクティブ検出モードは、ゾーンの定義時、またはゾーン検出の開始前後に設定できます。

1000 個を超える保留動的フィルタがある場合、Detector モジュールは次のように動作します。

- ゾーンを非アクティブにして自動検出モードで再度アクティブにするよう指示するエラー メッセージを表示する。
- ゾーンのログ　ファイルおよびレポートに推奨事項を記録してから、推奨事項を廃棄する。

新しい推奨事項が利用可能になっても、Detector モジュールは通知を表示しません。推奨事項を追跡するには、次のいずれかのタスクを行います。

- ゾーン設定モードで **show** コマンドを使用して、ゾーンのステータスを表示する。
- **event monitor** コマンドを使用して、新しい保留動的フィルタの作成時に通知を受け取る。
- 外部 syslog サーバを使用して、新しい保留動的フィルタの通知を受け取る。

いつでもインタラクティブ検出モードを停止して、自動検出モードに戻ることができます。Detector モジュールは、インタラクティブ検出モード中の決定をすべて無視し、現在のすべての保留動的フィルタを受け入れます。ポリシーは、動的フィルタを自動的に生成してアクティブにするという役割を再開します。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

インタラクティブ検出モードのアクティブ化

インタラクティブ検出モードを使用すると、攻撃の進行中に Detector モジュールが取るアクションを、より詳細に制御できます。インタラクティブ検出モードをアクティブにしない場合、Detector モジュールはゾーン上の攻撃を識別したときに動的フィルタを自動的にアクティブにします。

この項では、インタラクティブ検出モードで Detector モジュールをアクティブにするために必要な手順の概要を説明します。各手順には、タスクを完了するために必要な CLI コマンドが含まれています。

インタラクティブ検出モードをアクティブにするには、次の手順を実行します。

ステップ 1　**zone** *new-zone-name* **interactive** コマンドを使用して、インタラクティブ検出モードに設定された新しいゾーンを作成します。ゾーンがすでに存在する場合、このステップは省略してください。

```
user@DETECTOR-conf# zone scannet interactive
```

新しいゾーンを作成したら、ステップ 2 を省略してステップ 3 に進みます。

詳細については、P.10-6 の「インタラクティブ検出モードのゾーンの設定」を参照してください。

ステップ 2　インタラクティブ検出モードのゾーンの設定インタラクティブ検出モード用に設定されたゾーンがすでに作成されている場合は、このステップを省略します。

既存のゾーンをインタラクティブ検出モード用に設定するには、ゾーン設定モードで **interactive** コマンドを使用します。

```
user@DETECTOR-conf-zone-scannet# interactive
```

詳細については、P.10-6 の「インタラクティブ検出モードのゾーンの設定」を参照してください。

ステップ 3　（オプション）**event monitor** コマンドを使用すると、新しい推奨事項が使用可能になったときに Detector モジュールが通知を表示するように設定できます。

```
user@DETECTOR# event monitor
```

外部の syslog サーバを使用して、新しい保留動的フィルタの通知を受信することや、ゾーン設定モードで **show** コマンドを使用して、ゾーンのステータスを手動で表示することもできます。

ステップ 4　**learning** コマンドを使用して、Detector モジュールをアクティブにし、ゾーン トラフィック パターンをラーニングします。ラーニング プロセスの詳細については、第 8 章「ゾーン トラフィックの特性のラーニング」を参照してください。

ステップ 5　**detect** コマンドを使用して、ゾーン異常検出をアクティブにします。

```
user@DETECTOR-conf-zone-scannet# detect
```

詳細については、第 9 章「ゾーンのトラフィックの異常の検出」を参照してください。

ステップ 6　**show recommendations** コマンドを使用して、新しい推奨事項とその保留動的フィルタを表示します。

```
user@DETECTOR-conf-zone-scannet# show recommendations
user@DETECTOR-conf-zone-scannet# show recommendations 135
pending-filters
```

詳細については、P.10-7 の「推奨事項の表示」を参照してください。

ステップ 7　**recommendation** コマンドを使用して新しい推奨事項を管理する方法を決定します。これらの推奨事項を受け入れるか、無視するか、または自動的にアクティブ化することができます。

```
user@DETECTOR-conf-zone-scannet# recommendation 135 accept
```

詳細については、P.10-10 の「推奨事項の管理」を参照してください。

ステップ 8　**no interactive** コマンドを使用すると、インタラクティブ検出モードをいつでも非アクティブにできます。Detector モジュールは、新しい動的フィルタを自動的にアクティブにできます。

```
user@DETECTOR-conf-zone-scannet# no interactive
```

詳細については、P.10-13 の「インタラクティブ検出モードの非アクティブ化」を参照してください。

インタラクティブ検出モードのゾーンの設定

既存のゾーンのインタラクティブ検出モードをアクティブにするには、ゾーン設定モードで **interactive** コマンドを使用します。

次の例は、既存のゾーンに対してインタラクティブ検出モードをアクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# interactive
```

インタラクティブ検出モードに設定された新しいゾーンを作成するには、設定モードで次のコマンドを使用します。

zone *new-zone-name* **interactive**

new-zone-name 引数には、新しいゾーンの名前を指定します。ゾーン名は英数字の文字列とし、必ず英字で入力を開始してください。スペースは使用できません。また、63 文字以内で入力してください。

次の例は、新しいゾーンを作成し、インタラクティブ検出モードに設定する方法を示しています。

```
user@DETECTOR-conf# zone scannew interactive
```

インタラクティブ検出モードに設定された新しいゾーンが、デフォルト ゾーン テンプレートで作成されます。

推奨事項の表示

ゾーン設定モードで次のコマンドを入力すると、すべての推奨事項のリスト、保留動的フィルタのリスト、およびゾーンに固有の推奨事項を表示できます。

show recommendations [*recommendation-id*] [**pending-filters**]

表 10-1 に、**show recommendations** コマンドのキーワードと引数を示します。

表 10-1　show recommendations コマンドのキーワードと引数

パラメータ	説明
recommendation-id	（オプション）特定の推奨事項の ID。
pending-filters	（オプション）特定の推奨事項の保留フィルタのリストを表示します。

次の例は、すべての推奨事項のリストを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show recommendations
```

表 10-2 に、**show recommendations** コマンド出力のフィールドを示します。

表 10-2　show recommendations コマンド出力のフィールド説明

フィールド	説明
ID	推奨事項の識別番号。
Policy	推奨事項を作成したポリシー。
Threshold	超過したポリシーしきい値。
Detection date	推奨事項が作成された日時。
Attack flow	攻撃フローの特性。この特性には、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示しています。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。

表 10-2　show recommendations コマンド出力のフィールド説明（続き）

フィールド	説明
Min current rate	最小攻撃レート（パケット / 秒）。 複数の保留動的フィルタを持つ推奨事項の場合、保留動的フィルタの最小レートが表示されます。
Max current rate	最大攻撃レート（パケット / 秒）。 複数の保留動的フィルタを持つ推奨事項の場合、保留動的フィルタの最大レートが表示されます。
No. of pending-filters	ポリシーしきい値の超過が発生したために作成された保留動的フィルタの数。
Recommended action	推奨されるアクション。推奨事項を受け入れると、このアクションが実行されます。

特定の推奨事項の保留フィルタを表示する前に、すべての推奨事項とその ID のリストを表示するには、**show recommendations** コマンドを使用します。

表 10-3 に、**show recommendations pending-filters** コマンド出力のフィールドを示します。

表 10-3　show recommendations pending-filters コマンドのフィールド説明

フィールド	説明
ID	推奨事項の識別番号。
Policy	推奨事項を作成したポリシー。
Threshold	超過したポリシーしきい値（パケット / 秒）。
Pending-filter-id	保留動的フィルタの識別番号。
Detection date	推奨事項が作成された日時。
Attack flow	攻撃フローの特性。この特性には、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示しています。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。

表 10-3　show recommendations pending-filters コマンドのフィールド説明（続き）

フィールド	説明
Triggering rate	保留動的フィルタの作成をトリガーした攻撃レート（パケット / 秒）。
Current rate	現在の攻撃レート（パケット / 秒）。
Recommended action	推奨されるアクション。推奨事項を受け入れると、このアクションが実行されます。
Action flow	保留動的フィルタを受け入れた場合にそのフィルタで処理される、ゾーンへのトラフィック フローの特性。この特性には、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示しています。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。

Detector モジュールは、次の場合に、パラメータの 1 つにワイルドカードとしてアスタリスク（*）を使用できます。

- 値が特定されていない。
- パラメータに対して複数の値が測定された。

（注） Detector モジュールがインタラクティブ検出モードで、ゾーンに対する DDoS 攻撃が進行中である場合にだけ、推奨事項およびその保留動的フィルタを表示できます。

次の例は、推奨事項 135 の保留動的フィルタを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show recommendations 135
pending-filters
```

推奨事項の管理

推奨事項をアクティブにするかどうかを決定できます。すべての推奨事項、特定の推奨事項、または特定の保留動的フィルタに対して決定を行うことができます。その決定によって、ポリシーの保留動的フィルタが動的フィルタになるかどうか、およびその期間が決まります。

特定のポリシーの保留動的フィルタを自動的にアクティブにするよう Detector モジュールに指示できます。また、ポリシーによって推奨事項が生成されないよう Detector モジュールに指示することもできます。Detector モジュールのポリシーは、ゾーンがインタラクティブ検出モードで、DDoS 攻撃が進行中の場合、推奨事項を継続して生成します。ゾーンのステータスを検証して、さらにアクションが必要かどうかを判断するために推奨事項を管理する場合、ゾーンのステータスを表示することをお勧めします。

ゾーン ポリシーは、次のアクションを取ることができます。

- **notify**：ポリシーが Detector の syslog にイベントを記録します。イベントには、しきい値超過が発生したポリシーの詳細が記録されます。
- **remote-activate**：Detector が 1 つまたは複数のリモート Guard をアクティブにし、ゾーンの保護を開始します。

（注） 推奨事項を受け入れると、受け入れた推奨事項と同じまたは受け入れた推奨事項に含まれるフローを持ち、アクションとタイムアウトが同じである、その他の推奨事項も同様に受け入れられます。Detector モジュールは、これらの推奨事項を削除します。

ゾーンの推奨事項を決定するには、ゾーン設定モードで次のコマンドを使用します。

recommendation *recommendation-id* [**pending-filters** *pending-filter-id*] *decision* [*timeout*]

表 10-4 に、**recommendation** コマンドの引数とキーワードを示します。

表 10-4　recommendation コマンドの引数とキーワード

パラメータ	説明
recommendation-id	推奨事項の識別番号。アスタリスク（*）は、すべての推奨事項を示すワイルドカードです。
pending-filters *pending-filter-id*	（オプション）特定の保留動的フィルタの ID を指定します。
decision	推奨事項に対するアクション。指定できる値は、次のとおりです。 • **accept**：特定の推奨事項を受け入れます。保留動的フィルタは、動的フィルタになります。 • **always-accept**：特定の推奨事項を受け入れます。この決定は、推奨ポリシーによって新しい推奨事項が生成されると必ず、自動的に適用されます。保留動的フィルタは、自動的に動的フィルタになります。 このアクションを実行すると、Detector モジュールはこのような推奨事項を表示しなくなります。 • **always-ignore**：特定の推奨事項を無視します。動的フィルタも保留動的フィルタも生成されません。この決定は、ポリシーによって生成される将来のすべての推奨事項に自動的に適用されます。 推奨事項を常に無視するように決定した場合は、Detector モジュールが推奨事項を表示しなくなります。
timeout	（オプション）決定が適用される期間。指定できる値は、次のとおりです。 • **forever**：検出が有効である限り、推奨事項によって生成された動的フィルタをアクティブにします。このタイムアウトがデフォルトです。詳細については、P.6-22 の「動的フィルタの設定」を参照してください。 • *new-timeout*：定義した期間中、ポリシーによって生成された動的フィルタをアクティブにします。この期間は秒で測定されます。詳細については、P.6-22 の「動的フィルタの設定」を参照してください。

次の例は、推奨事項 135 を受け入れる方法を示しています。

```
user@DETECTOR-conf-zone-scannet# recommendation 135 accept
```

特定のポリシーまたはポリシーの任意の部分のインタラクティブ ステータスを設定し、ポリシーのその部分が推奨事項と保留動的フィルタを生成するかどうかを決定できます。ポリシーのインタラクティブ ステータスを設定することで、制御が可能になり、ポリシーをトラフィック フローによりよく適合させることができます。詳細については、P.7-32 の「ポリシーのインタラクティブ ステータスの設定」を参照してください。

Detector モジュールは、**always-accept** および **always-ignore** の推奨事項を表示しません。推奨事項を常に無視するまたは常に受け入れると決定した場合、その決定は、推奨事項を作成したポリシーのインタラクティブ ステータスの一部となります。

ポリシーをディセーブルまたは非アクティブにして、ポリシーが推奨事項と保留動的フィルタを生成しないようにすることができます。ポリシーをディセーブルまたは非アクティブにするには、**state** コマンドを使用します。詳細については、P.7-22 の「ポリシーの状態の変更」を参照してください。

次の例では、dns_tcp/53/analysis のインタラクティブ ステータスを **always-accept** に設定しています。

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/#
interactive-status always-accept
```

インタラクティブ検出モードの非アクティブ化

インタラクティブ検出モードを非アクティブにするには、ゾーン設定モードで **interactive** コマンドを使用します。ユーザがインタラクティブ検出モードを非アクティブにすると、Detector モジュールはすべての新しい動的フィルタを自動的にアクティブにし、ポリシーのインタラクティブ ステータスを **always-accept** に設定します（ゾーン ポリシーの表示方法の詳細については、P.7-39 の「ポリシーの表示」を参照してください）。

次の例は、ゾーン scannet のインタラクティブ検出モードを非アクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no interactive
```